DETECTING AND MITIGATING REGISTRAR COLLUSION IN DROP-ADD ACQUISITIONS OF DOMAIN NAMES

FIELD

[0001] The present disclosure relates generally to analyzing domain name acquisition requests submitted by domain name registrars to detect and mitigate potential drop-add collusion between the domain name registrars.

BACKGROUND

[0002] As Internet usage grows exponentially, the demand for Internet-related services is also growing rapidly. As a result of the increased usage of the Internet, the demand for domain names is also growing rapidly. Consequently, demand for domain-related services is also on the rise. Such domain-related services can include domain name creation, domain name registration renewal, and the like. Typically, a website serves as a primary vehicle for establishing an online presence for a domain name. To meet this ever increasing demand for domain name-related services, it is necessary that the entities that provide these services do so in an efficient and cost-effective manner.

[0003] The Domain Name System ("DNS") is the part of the Internet infrastructure that translates human-readable domain names into the Internet Protocol ("IP") numbers needed to establish Transmission Control Protocol ("TCP")/IP communication over the Internet. DNS allows users to refer to web sites, and other resources, using easier to remember domain names, such as "www.example.com", rather than the numeric IP addresses associated with a website, e.g., 123.4.56.78, and assigned to computers on the Internet. Each domain name can be made up of a series of character strings (e.g., labels) separated by dots. The rightmost label in a domain name is known as the top-level domain ("TLD"). Examples of well-known TLDs include .com, .net, .org, .edu, and .gov. Additional examples of TLDs include .biz, .info, and .name. Each TLD supports second-level domains, listed immediately to the left of the TLD, e.g., the "example" level in "www.example.com". Each second-level domain can include a number of third-level domains located immediately to the left of the second-level domain, e.g. the "www" level in www.example.com. The DNS registration system has also evolved to incorporate various country code TLDs ("ccTLDs"), each one reserved for use by a particular country, such as, .ca, .cn, and .us, associated with Canada, China, and the United States, respectively. The DNS and domain name registration system have also evolved to allow the use of alternative character sets to accommodate foreign languages.

[0004] The responsibility for operating each TLD, including maintaining a registry of the second-level domains within the TLD, is delegated to a particular organization, known as a domain name registry ("registry"). The registry is primarily responsible for answering queries for IP addresses associated with domains ("resolving"), typically through DNS servers that maintain such information in large databases, and operating its top-level domain. For most TLDs, in order to obtain a domain name, that domain name has to be registered with a registry through a DNS registrar, an entity authorized to register Internet domain names on behalf of end-users. Alternatively, an end-user can register a domain name indirectly through one or more layers of resellers. A registry may receive registrations from hundreds of registrars.

[0005] A registrar usually has a dedicated service connection with the registries in order to access domain-related services, e.g., domain name creation or renewal. Registrars typically use the Extensible Provisioning Protocol ("EPP") as a vehicle to communicate with the registries in order to register or renew domain names. EPP is a protocol designed for allocating objects within registries over the Internet. The EPP protocol is based on Extensible Markup Language ("XML"), which is a structured, text-based format. The underlying network transport is not fixed, although the currently specified method is over TCP.

SUMMARY

[0006] An authoritative domain name registry responsible for registering and resolving domain names associated with one or more TLDs can perform "domain drops" to release non-renewed domain names associated with the TLDs. Such domain drops can happen on a regular basis (e.g., daily at 2 PM Eastern Time) and can cause intense competition between domain name registrars, which can number in the hundreds or even thousands, to obtain certain non-renewed domain names. The registrars can make acquisition requests to obtain the non-renewed domain names within milliseconds of being dropped, with some acquisition requests failing because the non-renewed domain names have yet to be released (e.g., too early) or have been obtained by other registrars (e.g., too late). End-users (e.g., domainers, domain snipers, etc.) can contract services that attempt to obtain domain names on their behalf. These services can include the registrars directly or "drop-catch" services that leverage an undisclosed network of registrars to attempt domain name acquisition. For example, a registrar can spin off one or more subsidiary registrars to create such a network of registrars to improve their odd of obtaining just-dropped domain names.

[0007] Implementations of the present disclosure relate to systems and methods for analyzing the registrars' acquisition requests to detect and mitigate potential drop-add collusion between the registrars. An example drop-add collusion detection system can obtain information related to the acquisition requests from the registry, which can access the totality of the acquisition requests. By analyzing the acquisition requests to identify request patterns, the drop-add collusion detection system can detect the presence of and/or identify the undisclosed network of registrars performing drop-catch services in collusion.

[0008] In various implementations, the drop-add collusion detection system includes a collusion detector that can operate at or with the registry to obtain information related to acquisition requests submitted by the registrars attempting to acquire domain names in the registry's a drop pool of expired domain names. The collusion detector can provide attempt sets containing the domain names targeted by the registrars for acquisition, with each attempt set containing at least one targeted domain name that a respective registrar attempted to acquire via at least one acquisition request. The collusion detector can determine a degree of similarity between two or more attempt sets corresponding to a pair of the registrars, estimate a likelihood of collusion between the